epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION/DEPARTMENT OF TRANSPORTATION

Request for Comment on "Automated Driving Systems: A Vision for Safety"

Docket No. NHTSA-2017-0082

November 14, 2017

By notice published on September 23, 2016 the National Highway Traffic Safety Administration ("NHTSA") requests public comments on *Automated Driving Systems: A Vision for Safety*.[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments to explain why: (1) privacy is a matter of public safety; (2) NHTSA should promulgate mandatory rather than voluntary cybersecurity guidelines; and (3) the Federal Trade Commission's ("FTC") current enforcement regime is insufficient to protect driver privacy and security.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy and security. EPIC has worked extensively on the privacy and data security implications of connected cars.[2] EPIC has also submitted numerous comments to NHTSA on

[1] *Request for Comment on "Automated Driving Systems: A Vision for Safety,"* 82 Fed. Reg. 43321 (Nov. 14, 2017).
[2] EPIC Former Associate Director Khaliah Barnes, Testimony Before the U.S. House of Representatives, Committee on Oversight and Government Reform, Subcommittees on Information Technology and Transportation and Public

privacy issues raised by networked vehicles,[3] including comments on the Federal Automated Vehicle Policy.[4]

I. PRIVACY IS DIRECTLY RELEVANT TO MOTOR VEHICLE SAFETY

NHTSA has created a false dichotomy between privacy and cybersecurity by deciding to keep cybersecurity guidance but remove privacy guidance from the current Automated Driving Systems 2.0.[5] NHTSA's earlier Federal Automated Vehicle Policy[6] included a section devoted to privacy that is now absent. To explain this absence, NHTSA has stated that "privacy is not directly relevant to motor vehicle safety."[7] EPIC disagrees with this assessment.

Strong encryption in autonomous vehicles will be essential to driver safety. Encryption keeps communications and other information private, but it also keeps vehicle systems safe from hackers. Nearly all cars on the road today contain at least one wireless entry point ("WEP").[8] WEPs are essential to the functionality of built-in wireless features such as tire pressure

---

Assets, *The Internet of Cars* (Nov. 18, 2015), https://epic.org/privacy/edrs/EPIC-Connected-Cars-Testimony- Nov-18-2015.pdf; Brief of Amicus Curiae EPIC, *Cahen v. Toyota Motor Corporation*, No. 16-15496 (9th Cir. Aug. 5, 2016), https://epic.org/amicus/cahen/EPIC-Amicus-Cahen-Toyota.pdf; Marc Rotenberg, *Are Vehicle Black Boxes a Good Idea?*, THE COSTO CONNECTION (Apr. 2013), http://www.costcoconnection.com/connection/201304?pg=24#pg24; Marc Rotenberg, *Steer Clear of Cars That Spy*, USA TODAY (Aug. 18, 2011), http://usatoday30.usatoday.com/news/opinion/editorials/2011- 08-18-car-insurance-monitors-driving-snapshot_n.htm.

[3] *E.g.*, EPIC, Comments on the Federal Motor Vehicle Safety Standards: "Vehicle-to- Vehicle (V2V) Communications", Nat'l Highway Traffic Safety Admin., Docket No. NHTSA-2014-0022 (Oct. 20, 2014), https://epic.org/privacy/edrs/EPIC-NHTSA- V2V-Cmts.pdf; EPIC et al., Comments on the Federal Motor Vehicle Safety Standards; Event Data Recorders, Nat'l Highway Traffic Safety Admin., Docket No. NHTSA- 2012-0177 (Feb. 11, 2013), https://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR- Cmts.pdf; *see generally* EPIC, *State Auto Black Boxes Policy* (2015), https://epic.org/state-policy/edr/; EPIC, *Automobile Event Data Recorders (Black Boxes) and Privacy* (2015), https://epic.org/privacy/edrs/.

[4] EPIC, Comments on the *Federal Automated Vehicle Policy*, Nat'l Highway Traffic Safety Admin., Docket No. 2016-22993 (Nov. 22, 2016), https://epic.org/apa/comments/EPIC-NHTSA-AV-Policy-comments-11-22-2016.pdf/.

[5] https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[6] Nat'l Highway Traffic Safety Admin., *Federal Automated Vehicle Policy*, 81 Fed. Reg. 65,703, https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/federal_automated_vehicles_policy.pdf.

[7] https://www.nhtsa.gov/manufacturers/automated-driving-systems#automated-driving-systems-topic

[8] *See Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*, Sen. Edward J. Markey (D-Mass) (Feb. 2015), https://www.markey.senate.gov/imo/media/doc/2015-02- 06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

monitoring systems, Bluetooth, keyless entry, anti-theft systems, and navigation.[9] However, WEPS also provide entry points for remote vehicle hacking. A 2011 report by computer scientists showed how a hacker could use WEPs to "take control of various features – like the car locks and brakes – as well as to track the vehicle's location, eavesdrop on its cabin and steal vehicle data."[10]

In a 2013 study, researchers Charlie Miler and Chris Valasek connected laptops to the computer systems of a Toyota Prius and a Ford Escape and were able to jerk the wheel at high speeds, turn the car, cause sudden acceleration or braking, turn on the horn, tighten the seatbelts in anticipation of a nonexistent crash, and kill the breaks.[11] In 2015, those same researchers were able to wirelessly hack a Jeep Cherokee traveling on a highway ten miles away from their computers.[12] The researchers were able to manipulate the air conditioning, turn on the radio, activate the windshield wipers and wiper fluid, take over the car's digital display screen, cut the transmission, kill the engine, and engage and disable the breaks.[13] The same researchers were able to control steering of the Jeep Cherokee and activate the safety brake while the vehicle was travelling at high speeds.[14]

---

[9] *Id.*
[10] John Markoff, *Researchers Show How a Car's Electronics Can Be Taken Over Remotely*, N.Y. Times (Mar. 9, 2011), http://www.nytimes.com/2011/03/10/business/10hack.html.
[11] Dr. Charlie Miller & Chris Valasek, *Adventures in Automotive Networks and Control Units*, IOActive (2014) http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and _Control_Units.pdf; Steve Henn, *With Smarter Cars, The Doors Are Open To Hacking Dangers*, NPR (July 30, 2013), http://www.npr.org/sections/alltechconsidered/2013/07/30/206800198/Smarte r-Cars-Open-New-Doors-To-Smarter-Thieves.
[12] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me in It*, WIRED (July 21, 2015), https://www.wired.com/2015/07/hackers-remotelykill-jeep-highway/.
[13] *Id*.
[14] Adam Greenberg, *The Jeep Hackers Are Back To Prove Car Hacking Can Get Much Worse*, WIRED, Aug. 1, 2016, https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/.

While researches and scientists have done most of the reported hacks on moving cars in controlled setting, wide scale malicious car hacking is certainly imminent.[15] Thieves can already hack computer-based door lock systems to rob parked cars.[16] And in 2010, a disgruntled former car salesman disabled more than one hundred cars in Austin, Texas by hacking into a "web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments."[17]

The very real possibility of remote car hacking poses substantial risks to driver safety and security. Cars can be remotely hacked from anywhere in the world via the internet.[18] Wireless hacking can give hackers access to the cars physical location which would facilitate crimes such as harassment, stalking, and car theft.[19]

The privacy of geolocation data also raises serious public safety concerns. Stalkers and domestic abusers may exploit geolocation data to track down their victims. Recently, a man used Snapchat's geolocation features to follow his girlfriend. He found her in a car with another man and stabbed him.[20] Armed robbers used geolocation data from the Pokémon Go app to find their

---

[15] *See, e.g.* Alex Hern, *Fiat Chrysler recalls 8,000 more Jeeps over wireless hacking*, The Guardian (Sept. 7, 2015), http://www.theguardian.com/technology/2015/sep/07/fiat-chrysler-recalls- more-jeeps-wireless-hacking; Reem Nasr, *Fiat Chrysler recalling 1.4M vehicles amid hacking defense*, CNBC (July 24, 2015), http://www.cnbc.com/2015/07/24/fiat- chrysler-recalling-14m-vehicles-amid-hacking-defense.html; Miller & Valasek *supra* note 19.; Charlie Osborne & Zero Day, *Your Car Will Be Recalled in 2017 Thanks To Poor Open Source Security*, ZDNET, Nov. 21, 2016, http://www.zdnet.com/article/2017-the-year-hacking-will-force-your-car-to-be-recalled/.

[16] Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), http://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[17] Kevin Poulsen, *Hacker Disables More Than 100 Cars Remotely*, WIRED (Mar. 17, 2012), https://www.wired.com/2010/03/hacker-bricks-cars/.

[18] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me in It*, WIRED (July 21, 2015), https://www.wired.com/2015/07/hackers-remotelykill-jeep-highway/.

[19] *Id*. *See also* Bruce Schneier, *The Internet of Things Will Turn Large-Scale Hacks Into Real World Disasters*, MOTHERBOARD, Jul. 25, 2016, https://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster.

[20] Mike Murphy, *A man reportedly stabbed his girlfriend's lover after tracking her on Snapchat*, Quartz (Nov. 6, 2017), https://qz.com/1121867/a-man-reportedly-stabbed-his-girlfriends-lover-after-tracking-her-on-snapchats-snap-maps/.

victims.[21] It was not the security of the data that put people at risk; the criminals did not hack Snapchat or Pokémon Go. Rather, it was the privacy practices of the apps that allowed geolocation data to be exploited. Automated vehicles will likely have features that similarly expose users' precise geographic location that puts them in danger.

Without privacy standards regulating employee access to user data, there will be abuses that could endanger the public. Company employees often abuse their authorized access to user data. For example, Uber—one of the leading companies developing autonomous vehicles—has a history of abusing the location data of its customers. Individual employees could use "God View," an "easily accessible" internal company tool, to obtain a specific user's real-time and historic location, tracking a user in real time.[22] Top Uber executives tracked journalists writing pieces critical of the company.[23] The sensitivity of the data collected by vehicle companies makes this a safety concern. A Ford executive stated in 2014, "We know everyone who breaks the law, we know when you're doing it. We have GPS in your car, so we know what you're doing."[24] Unfettered access to such information could put members of the public at risk. Privacy standards governing proper internal uses would help limit abuses of sensitive information.

Far too many companies collect, use, and disclose detailed personal information without following proper procedures for safeguarding that information. Our government must respond with comprehensive, baseline privacy protections that ensure Fair Information Practices – an

[21] Alan Yuhas, *Pokémon Go: armed robbers use mobile game to lure players into trap*, The Guardian (July 11, 2016), https://www.theguardian.com/technology/2016/jul/10/pokemon-go-armed-robbers-dead-body.
[22] EPIC Complaint

[23] *Id.*

[24] Eugene Volokh, "Ford 'Know[s] Everyone Who Breaks the Law' Using Cars They Made—Why Aren't They Doing Something about It?," *Volokh Conspiracy*, January 10, 2014, http://www.volokh.com/2014/01/10/ford -knows-everyone-breaks-law-using-cars-made-arent-something.

internationally recognized set of informational privacy practices[25] – are applied to autonomous vehicles.

II. VOLUNTARY GUIDANCE IS INSUFFICIENT

Although *Automated Driving Systems: A Vision for Safety* does not contain privacy guidance, it does contain cybersecurity guidance. However, the guidance is voluntary and is missing oversight and enforcement mechanisms. Automotive vehicle manufacturers are given a range of things that they *should* do, but not that they *must* do. Leaving essential security protections to the discretion of carmakers and companies places consumers at risk. EPIC urges NHTSA to implement mandatory privacy protections for automated vehicles as soon as possible.

The Automated Vehicles Policy should include meaningful oversight and enforcement mechanisms. Without enforcement mechanisms, consumers have no recourse if companies do not abide by NHTSA's guidance. NHTSA and the Department of Transportation ("DOT") should enforce privacy safeguards and security standards for automated vehicles.

Meaningful enforcement of privacy and security protections also requires a private right of action against companies who misuse and fail to secure personal information. Private rights of actions are familiar remedies in U.S. privacy law and would be appropriate in the context of automated vehicles.[26]

III. THE FTC's CURRENT APPROACH IS TOO WEAK

The FTC is ill-equipped to handle the scale of the privacy and security challenges faced by today's consumers. NHTSA answered the frequently asked question—"What is NHTSA's

[25] *See* EPIC, *Code of Fair Information Practices*, https://www.epic.org/privacy/consumer/code_fair_info.html.
[26] *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012); Fair Debt Collection Practices Act, 15 U.S.C. §§ 1692–1692p; Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508; 100 Stat. 1848.

approach to privacy?"—by stating that it was the FTC's responsibility to protect to consumer privacy rather than the Department of Transportation's or NHTSA's responsibility.[27] But the FTC's authority to bring enforcement actions for unfair and deceptive practices does not preempt NHTSA's ability to regulate the privacy and security of vehicles.

At this time, the FTC is simply not doing enough to safeguard the personal data of American consumers. While we respect the efforts of the Commission to protect consumers, the reality is that the FTC lacks the statutory authority, the resources, and the political will to adequately protect the privacy of American consumers. Relying on the FTC to address all consumer privacy concerns is not in the best interest of consumers.

The FTC's privacy framework – based largely on "notice and choice"– is simply not working. Research shows that consumers rarely read privacy policies; when they do, these complex legal documents are difficult to understand. Nor can industry self-regulatory programs provide realistic privacy protections when they are not supported by enforceable legal standards.

Even when the FTC reaches a consent agreement with a privacy-violating company, the Commission rarely enforces the Consent Order terms.[28] American consumers whose privacy has been violated by unfair or deceptive trade practices do not have a private right of action to obtain redress. Only enforceable privacy protections create meaningful safeguards, and the lack of FTC enforcement has left consumers with little recourse.

Fundamentally, the FTC is not a data protection agency. Without regulatory authority, the FTC is limited to reactive, after-the-fact enforcement actions that largely focus on whether

[27] https://www.nhtsa.gov/manufacturers/automated-driving-systems#automated-driving-systems-topic
[28] *See EPIC v. FTC*, No. 12-206 (D.C. Cir. Feb. 8, 2012).

companies honored their own privacy promises. Because the United States currently lacks comprehensive privacy legislation or an agency dedicated to privacy protection, there are very few legal constraints on business practices that impact the privacy of American consumers.

IV. CONCLUSION

Automated Driving Systems: A Vision for Safety does not further NHTSA's mission of protecting drivers. New vehicle technologies offer a variety of beneficial services to American drivers, and are being quickly implemented by car manufacturers. But these new technologies also raise substantial privacy and safety concerns that must be addressed through meaningful, legally enforceable safeguards. Current approaches, based on industry self-regulation, are inadequate and fail to protect driver privacy and safety. NHTSA must issue mandatory rules to address the myriad risks posed to drivers operating vehicles in the United States.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

/s/ *Christine Bannan*
Christine Bannan
EPIC Policy Fellow